

## **REMARKS**

In the Office Action dated August 18, 2004, informalities in claims 8, 10 and 11 were noted, all of which have been corrected. Additionally, Applicants noted an incorrect statement in the specification at page 4, and a typographical error at page 5, both of which have been corrected.

Claims 1 and 5-8 were rejected under 35 U.S.C. §103(a) as being unpatentable over Ryan, Jr. et al in view of Davies, Jr. et al. Claims 2 and 3 were rejected under 35 U.S.C. §103(a) as being unpatentable over Ryan, Jr. et al and Davies, Jr. et al, further in view of Wiley et al. Claims 9-11 were rejected under 35 U.S.C. §103(a) as being unpatentable over Ryan, Jr. et al and Davies, Jr. et al, further in view of Mori et al. Claims 12 and 13 were rejected under 35 U.S.C. §103(a) as being unpatentable over Ryan, Jr. et al and Davies, Jr. et al, further in view of Fang et al.

Applicants note with appreciation that claim 4 was stated to be allowable if rewritten in independent form. In view of Applicants belief that claim 1 as amended above is patentable over the references relied upon by the Examiner, claim 4 has been retained in dependent form at this time.

In many types of devices wherein security data are stored in a protected module (security module). In order to avoid the security data from being compromised or accessed by a tamperer, the security data are voltage-supported, so that unauthorized removal of the security module from the motherboard, for example, automatically causes erasure of the security data. This also means, however, that protective measures must be taken to avoid loss of the data in the security module during events that do not constitute an effort at tampering, such as

loss of line voltage. Normally, the security module is supplied, like all of the other components, with voltage from the mains. Conventionally, a security module is provided with a battery contained within the security module that supplies the necessary voltage to avoid loss of data during a temporary voltage outage. Since the security module, by its very nature, must be made as mechanically tamper-proof as possible, if and when the battery within the security module must be replaced, due to frequent usage or simply due to the battery becoming drained over a longer period of time, this presents difficulties. This is explained in the last paragraph of page 3 of the present specification.

The subject matter disclosed and claimed in the present application overcomes these problems by providing another battery that is located outside of the secured region (i.e. outside of the security module). It is this battery that is used as the primary back-up power source in the event of a power outage, for example. A battery within the security module is still retained, however this battery is called upon to supply power to the components in the security module only when the battery outside of the security region is unable to do so, such as by virtue of becoming drained or during replacement thereof.

Independent claim 1 has been amended to make clear that the components in the security module are normally supplied with voltage from a mains voltage, and the "second battery" is the battery that supplies power to the security components in the event of a line voltage failure. The "first battery" has been stated to supply power to the security components only when the second battery is unable to do so.

The Ryan, Jr. and Davies, Jr. et al references, even in combination, do not disclose or suggest such an arrangement.

The Ryan, Jr. et al reference is not concerned with providing backup power to components in an encryption circuit in the event of a failure of the line voltage. The charged capacitor C1 in the Ryan, Jr. et al circuit is used to supply power to the encryption circuit for a completely different purpose, namely to avoid determining cryptographic secrets by means of Differential Power Analysis (DPA), as explained at column 4, lines 20-25 of the Ryan, Jr. et al reference. DPA involves monitoring fluctuations in the line that supplies power to an encryption circuit for the purpose of detecting details of the operation of the encryption circuit. This problem exists no matter what type of power source is used as the "normal" power source to the encryption circuit, as long as the power is supplied via an unprotected cable or wire.

The circuit disclosed in the Ryan, Jr. et al reference solves this problem by recognizing that during the brief times that an encryption circuit is actually performing encryption operations, it can be powered by the capacitor C1, which is contained within the secured region and therefore the power supply line between the capacitor C1 and the encryption circuit is not accessible from outside of the secured region. The transistor Q1 is used to switch power supply from the external source to the capacitor C1 under those circumstances.

The Examiner has characterized the capacitor C1 in the Ryan, Jr. et al reference as a "battery," (a characterization with which Applicants disagree), but has acknowledged that the external "power source" in the Ryan, Jr. et al reference is not a battery. The Examiner relied on the Davies, Jr. et al reference as disclosing the use of a back-up battery for a security module. The Examiner has proposed using a battery of the type described in the Davies, Jr. et al reference in place of the power source in the Ryan, Jr. et al reference. For the reasons discussed above, however,

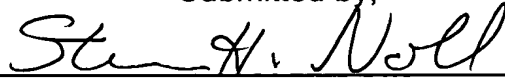
this would serve no purpose in the Ryan, Jr. et al reference, since there is no "back-up" power supply that is employed in the Ryan, Jr. et al reference. A battery connected at the location of the power source in the Ryan, Jr. et al reference would still be susceptible to DPA, since it would have to be connected to the encryption circuit via the unprotected power supply line. Modifying the Ryan, Jr. et al reference to employ a battery instead of a power source, therefore, would be purely arbitrary, and would serve no improving function with regard to the operation of the Ryan, Jr. et al circuit.

Moreover, in view of the amendments to independent claim 1, a clear differentiation is made among the power supply from the mains voltage, and the first battery and the second battery. Even if the Ryan, Jr. et al circuit were modified in accordance with the teachings of Davies, Jr. et al as proposed by the Examiner, an arrangement as set forth in claim 1 still would not result.

Claim 1, therefore, would not have been obvious to a person of ordinary skill in the field of security module design and operation based on the teachings of Ryan, Jr. et al and Davies, Jr. et al. Dependent claims 2, 3 and 5-13 add further structure to the non-obvious combination of claim 1, and are therefore patentable over the teachings of the references of record for the same reasons discussed above in connection with claim 1.

All claims of the application are therefore submitted to be in condition for allowance, and early reconsideration of the application is respectfully requested.

Submitted by,



(Reg. 28,982)

---

SCHIFF, HARDIN LLP  
**CUSTOMER NO. 26574**  
Patent Department  
6600 Sears Tower  
233 South Wacker Drive  
Chicago, Illinois 60606  
Telephone: 312/258-5790  
Attorneys for Applicants.

CH1\ 4195440.1